N80-21378

ORIGINAL PAGE IS
OF POOR QUALITY

A Fast Algorithm for Encoding the (255,223) Reed-Solomon Code Over GF(2^8)

R. L. Miller and T. K. Truong
Communications Systems Research Section

I. S. Reed
University of Southern California

A new scheme for reducing the numerical complexity of the standard Reed-Solomon (R-S) encoding algorithm is developed. As an example, the encoding of a (255,223) R-S code (NASA standard for concatenation with convolutional codes) is shown to require 75 percent fewer multiplications and 61 percent fewer additions than the conventional method of computation.

I. Introduction

In this article, the fast syndrome method developed in Ref. 1 and Lagrange interpolation are used to develop a fast algorithm for encoding R-S codes. It is shown that both the number of multiplications and additions of this new scheme is substantially fewer than is required by the conventional encoding techniques.

An advantage of this new algorithm aside from speed is that its first step consists of performing a syndrome-like calculation, which can be implemented by using the existing syndrome algorithm used in the decoder. This fact can be used to lower the total hardware cost of the encoder-decoder system.

II. Encoding Procedure

Let $n = 2^m - 1$ be the block length of an R-S code of designed distance d in $GF(2^m)$. The number of m-bit message symbols is $k = n - d + 1$.

To encode the k information symbols into an $n = 2^m - 1$ symbol R-S code word, one first defines the generator polynomial

$$G(x) = \prod_{i=1}^{d-1} (x - \alpha^i)$$

when α is a primitive nth root of unity. The code consists of all multiples of $G(x)$, subject to the constraint that $x^n = 1$.

Let a_i for $d - 1 \leqslant i \leqslant n - 1$ be the message symbols, and define

$$I(x) = \sum_{i=d-1}^{n-1} a_i x^i$$

In order to generate the code word with information symbols corresponding to $I(x)$, proceed as follows: let

$$I(x) = Q(x)G(x) + R(x) \quad (1)$$

where $Q(x)$ is a quotient polynomial, $G(x)$ is the generator polynomials, and $R(x)$ is the remainder upon dividing $I(x)$ by $G(x)$. Finally, $I(x)$ is encoded into

$$C(x) = I(x) - R(x) \quad (2)$$

The new encoding procedure of an R-S code is composed of the following two steps:

(1) Compute $I(\alpha^i)$ for $1 \leqslant i \leqslant d-1$ by the technique which is used to compute syndromes in the decoder. Note that by Eq. (2), $I(\alpha^i) = R(\alpha^i)$ for $1 \leqslant i \leqslant d-1$.

(2) Compute $R(x)$ from $R(\alpha^i)$ using Lagrange interpolation

$$R(x) = \sum_{i=1}^{d-1} R(\alpha^i) E_i(x)$$

where $E_i(x)$ is defined by

$$E_i(x) = \frac{\prod_{j \neq i} (x - \alpha^j)}{\prod_{j \neq i} (\alpha^i - \alpha^j)} \text{ for } 1 \leqslant i \leqslant d-1 \quad (3)$$

The degree of $E_i(x)$ is $d-2$; hence, the degree of $R(x)$ is at most $d-2$. Thus, the parity symbols consist of the $d-1$ coefficients of $R(x)$, as desired. Note that a direct computation of $R(x)$ in Eq. (1) involves $(d-1)\cdot(n-d+1)$ multiplications and $(d-1)\cdot(n-d+1)$ additions. If one uses a fast syndrome calculation, say, for the case $n = 255$, $k = 233$, it is shown in the following example that the encoder requires only 1812 multiplications and 2764 additions instead of the 7136 multiplications and 7136 additions required by a more conventional computation. This results in a significantly faster encoding scheme.

Example

Let $n = 255$ be the block length of an R-S code of designed distance $d = 33$ over $GF(2^8)$. This code will correct any combination of 16 or fewer symbol errors. The first step of the encoding process is to compute $I(\alpha^i)$ for $1 \leqslant i \leqslant 32$. That is,

$$I(\alpha^j) = \sum_{i=0}^{255-1} a_i \alpha^{ij} \text{ for } 1 \leqslant j \leqslant 32 \quad (4)$$

where α is an element of order 255 in $GF(2^8)$, and $a_i = 0$ for $0 \leqslant i \leqslant 31$. Note that Eq. (4) is the same formula as Eq. (1) in Ref. 1. Thus, using the same computing procedure, one obtains $I(\alpha^j)$ for $1 \leqslant j \leqslant 32$. It follows from Ref. 1 that the total number of multiplications and additions needed to compute the $I(\alpha^i)$ for $1 \leqslant j \leqslant 32$ is 852 and 1804, respectively. The second step of the encoding process is to compute $R(x)$ defined in Eq. 3, i.e.,

$$R(x) = \sum_{i=1}^{32} R(\alpha^i) E_i(x) \quad (5)$$

Since $E_i(x)$ can be pre-computed, $32 \times 30 = 960$ multiplications and 960 additions are needed to compute $R(x)$. Hence, the total number of multiplications and additions required for encoding is $852 + 960 = 1812$ and $1804 + 960 = 2764$, respectively. In contrast, the total number of multiplications and additions for encoding by conventional methods is $223 \times 32 = 7136$ each.

Acknowledgment

The authors wish to thank Prof. J. Massey of the Electrical Engineering Department, University of California, Los Angeles, for suggesting the possibility of a fast encoding algorithm of the type presented in this paper.

Reference

1. Truong, T. K., Miller, R. L., and Reed, I. S., "A Fast Technique for Computing Syndromes of BCH and R-S Codes," *Electronics Letters*, Vol. 15, No. 22, pp. 720-721, October 25, 1979.

Maximum CW RFI Power Levels for Linear Operation of the DSN Block IV Receiver at S-Band Frequencies

D. R. Hersey and M. K. Sue
Telecommunications Systems Section

This article describes the results of a study performed to determine the maximum allowable CW RFI power into the DSN S-band maser to ensure linear amplification of the desired signal by the maser and Block IV receiver.

I. Introduction

The power levels of CW signals that result in gain compression of the S-band maser at various frequencies has been well defined (Ref. 1). It has been generally assumed that the maser will saturate at weaker power levels than stages in the receiver, and, consequently, the criterion for avoiding receiver saturation by CW radio frequency interference (RFI) was the maser saturation curve of Fig. 1.

In this study the most sensitive points within the Block IV receiver were considered along with the maser saturation characteristics. A curve was developed to show maximum allowable CW interference power into the maser versus signal frequency to ensure linear operation of the receiver.

It should be pointed out that many circuit parameter specifications which adequately ensure that the receiver meets its design requirements (i.e., properly receives the desired signal) do not provide sufficient information for determining the worst-case parameter values for RFI analyses. For example, the minimum gain of an amplifier is specified but the maximum gain of the amplifier, which causes the worst case RFI effect, is not. Because the worst-case values of many parameters could not be determined, it was necessary to use typical and minimum specified values in this study. As a result, the actual levels required to cause nonlinear operation of the receiver may vary from receiver to receiver and from the curve developed herein. It is estimated that the magnitude of this variation is typically 3 dB.

II. Model Description

The model for maximum allowable CW RFI at S-band is given in Appendix A and shown graphically by Fig. 5. This analytic model is based upon the following assumed receiver settings and conditions:

(1) The design point tracking loop noise bandwidth ($2B_{Lo}$) is 10 Hz.

(2) The predetection bandwidth is 20 kHz.

(3) The system noise temperature is 23 K.

(4) The signal level control is set at 20 dB.

(5) The receiver is locked to a desired signal having a power level of −165 dBm (−195 dBW) at the maser input (this signal level corresponds to the minimum 10-dB SNR in $2B_{Lo}$ recommended by the DSN).

Shown in Fig. 2 is a simplified block diagram of the Block IV receiver. The circled numerals denote circuit points where signal power must not exceed certain limits to ensure linear operation. The maximum allowable power levels at these points are determined by module characteristics, and by the overall gain and frequency response of the receiver stages preceding the circuit point (see Appendix B). These values are given in Table 1. The first row of Table 1 contains the module limits that are power levels which, if exceeded, will cause the stage associated with the point to operate in a nonlinear region. The subsequent entries in the table show the corresponding power at each preceding point when the most sensitive circuit points are consecutively set to their module limits.

As an example of the use of the table, consider the case when point 7 is set to its module limit. From the table it is seen that the maser input signal necessary to cause the limit value (+20 dBm) at point 7 is -90 dBm. From Fig. 1, it is found that the maser limit value at frequencies within ±4 MHz of the desired signal is -90 dBm, and, therefore, it is seen that the telemetry output (point 7) and maser will saturate at the same receiver input power.

To present the analytical model graphically, first, the maximum allowable power at the preselector input (from Table 1) was plotted versus interfering signal frequency in Fig. 3. The points enclosed in circles and triangles are measured saturation values which are discussed in the following section.

Since the receiver preselector has a much wider bandwidth (140 MHz) than the maser (30 MHz), Fig. 3 must be corrected for the maser frequency response. This plot is shown in Fig. 4.

Next, the maser saturation characteristics curve (Fig. 1) is combined with Fig. 4 to obtain the overall receiver saturation curve shown in Fig. 5. Figures 3, 4, and 5 are all drawn showing the receiver locked to a single desired carrier signal, as it would be at any given time. To define the susceptibility, taking into account that the receiver can be tuned to any frequency within the DSN S-band downlink receive band (2290 to 2300 MHz), the most sensitive region of the curve would be drawn 10 MHz wide (from 2290 to 2300 MHz).

III. Verification Tests

Verification of the model was accomplished by testing the Block IV receiver without the maser and combining the results with empirical maser saturation data obtained from the reference. Identical tests were performed in CTA 21, using an operational receiver, and in the Telecommunications Development Laboratory (TDL), which has the Engineering Model Block IV receiver.

The test configuration is shown in Fig. 6. The spectrum analyzer is used to measure the suppression of the desired signal caused by the interfering signal applied at the preselector input. This analyzer provides a 1-Hz resolution bandwidth, which allows accurate measurement of the signal power at low signal-to-noise ratios. Because the instrument (HP Model 3580) is limited to frequencies of 50 kHz or less, down conversion of the 10-MHz and 100-kHz outputs was necessary. The attenuator used before the mixer is required to prevent the test mixer from being saturated by the interfering signal power at the 10-MHz distribution amplifier and 100-kHz IF amplifier outputs. The test accuracy is estimated to be ±4 dB.

The results of these tests are shown in Fig. 3. The TDL test results, shown by circled points, show good agreement with the model from 2260 to 2310 MHz. Deviations from the model outside this range were caused by the TDL's 325-MHz IF amplifier, which is of a different design than the DSN operational amplifier.

The CTA 21 points show good agreement with the model, except the points at 2330 and 2340 MHz show that the preselector bandwidth of CTA 21's receiver is approximately 4 MHz wider than assumed by the model.

Saturation characteristics of the 100-kHz IF amplifier at frequencies within the predetection bandwidth could not be measured directly. In this region, severe tracking performance degradation will occur before saturation takes place (tracking loop performance in the presence of a CW RFI will be discussed in future reports). Instead, the gain and output 1-dB compression point of the 100-kHz IF amplifier were measured and found to agree with the model assumed values (42 dB and +7 dBm, respectively).

IV. Conclusions

The test results show that the receiver only saturation model (Fig. 3) is sufficiently accurate to use in developing the overall receiver saturation curve (Fig. 5). This model predicts that the 10-MHz outputs to telemetry and ranging will saturate at nearly the same power level as the maser when the interfering signal frequency is within ±4 MHz of the desired signal frequency. Outside of this region the maser saturation characteristics will predominate.

Within ±10 kHz of the desired signal, it is known that severe carrier tracking degradation will occur at much lower levels of interfering signal power than that which will produce

saturation of the 100-kHz IF amplifier linear output. Modeling of the carrier tracking degradation produced by CW interference is currently underway. This model and verification test results will be the subject of a future article.

Reference

1. Clauss, R. C., "X- and K-Band Maser Development: Effects of Interfering Signals," *Deep Space Network Progress Report 42-42*, pp. 85-87, Jet Propulsion Laboratory, Pasadena, CA, Dec. 15, 1977.

Table 1. Maximum CW power levels to ensure linear receiver operation

Condition	Maximum CW power, dBm								
	Circuit point								
	1	2	3	4	5	6	7	8	9
Module limit	See Fig. 1	–	−7	−39	+10	−18	+20	−5	+7
For limit value at circuit point 9 for interfering frequencies within ±10 kHz of desired signal frequency	−133	−85	−87	−94	−39	−68	−23	−35	+7
For limit value at circuit point 7 for interfering frequencies within ±4 MHz of desired signal frequency	−90	−42	−44	−51	+4	−25	+20	–	–
For limit value at circuit point 6 for interference signals within ±15 MHz of desired signal frequency	−83	−35	−37	−44	+11	−18	–	–	–
For limit value at circuit point 5 for interfering frequencies within ±36 MHz of desired signal frequency	−84	−36	−38	−45	+10	–	–	–	–
For limit value at circuit point 4 for interfering frequencies between 2182 and 2322 MHz	−78	−30	−32	−39	–	–	–	–	–

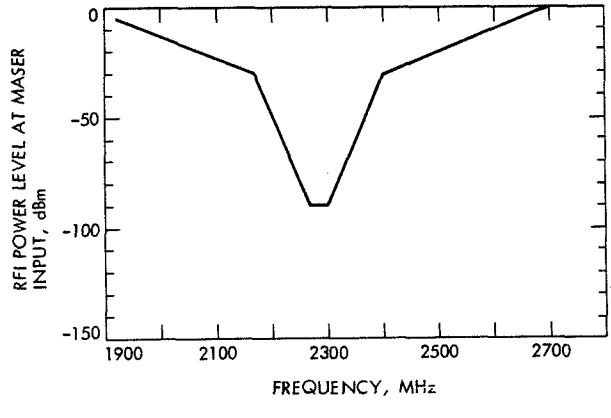
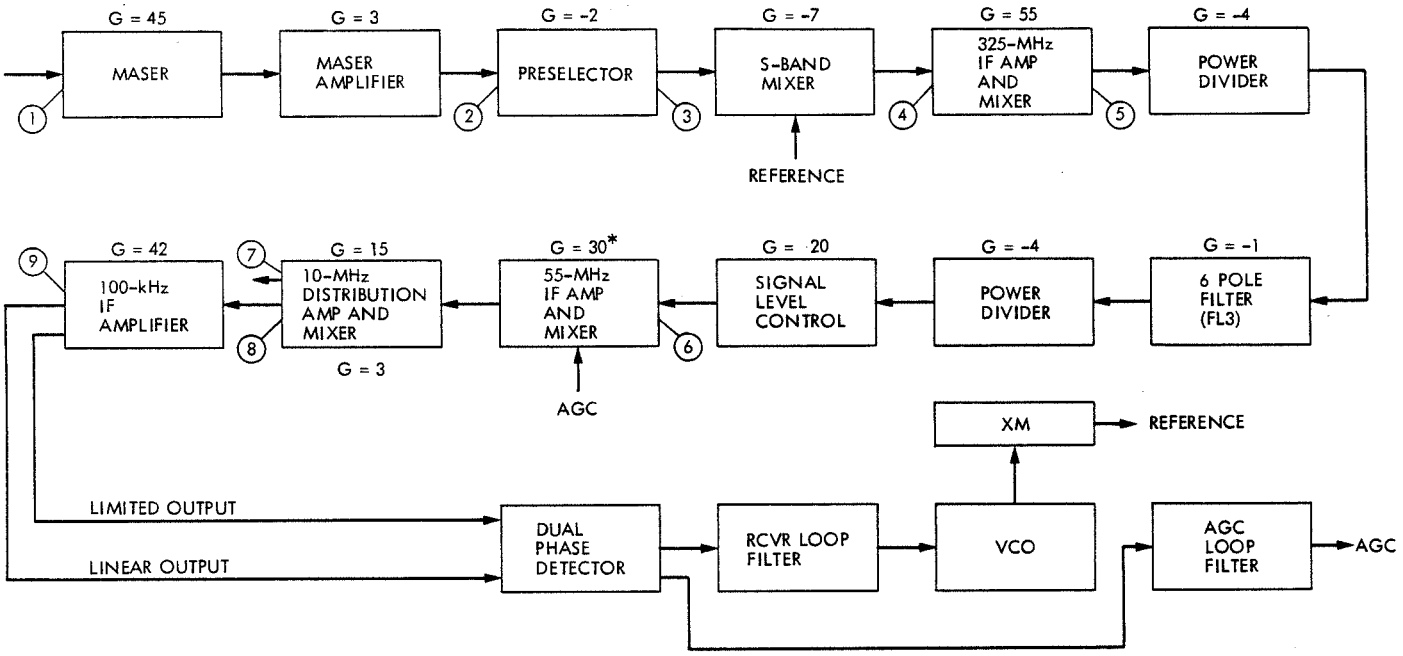


Fig. 1. Maximum allowable CW RFI power to prevent S-band maser saturation (1 dB or less gain compression)



*FOR -165 dBm DESIRED SIGNAL INTO MASER

Fig. 2. Simplified Block IV receiver block diagram, S-band

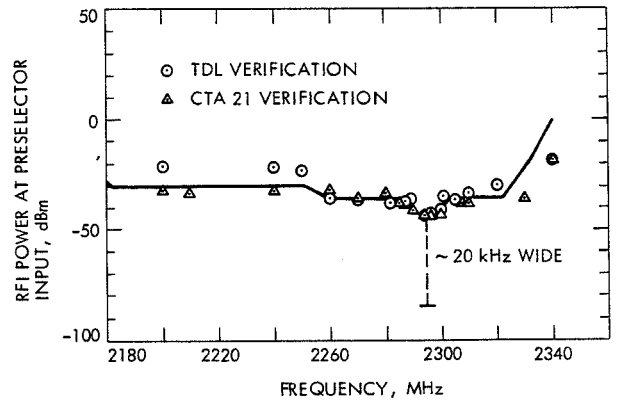


Fig. 3. Maximum CW RFI power into Block IV receiver (only) for 1 dB or less gain compression (receiver locked to S-band channel 14)

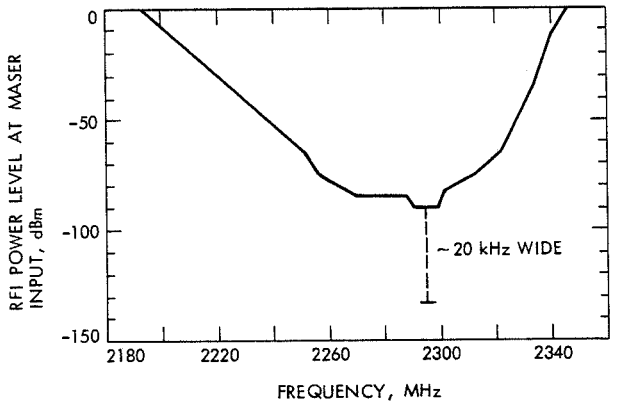


Fig. 4. Maximum allowable CW RFI power into maser to prevent saturation of Block IV receiver (only) operating at S-Band channel 14

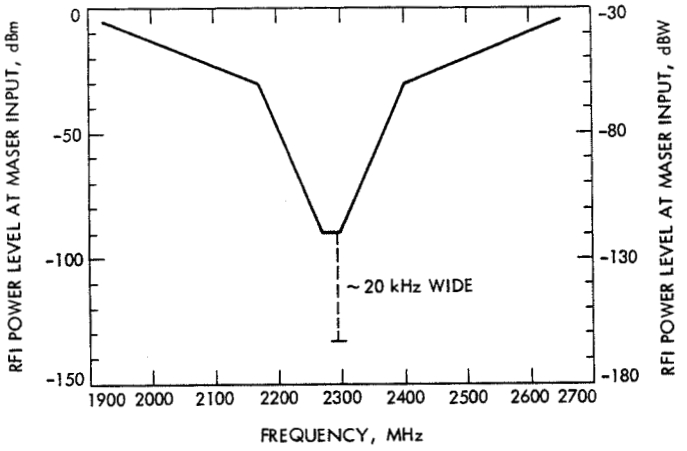


Fig. 5. Maximum allowable CW RFI power into S-band maser for 1 dB or less gain compression of maser or Block IV receiver operating at channel 14

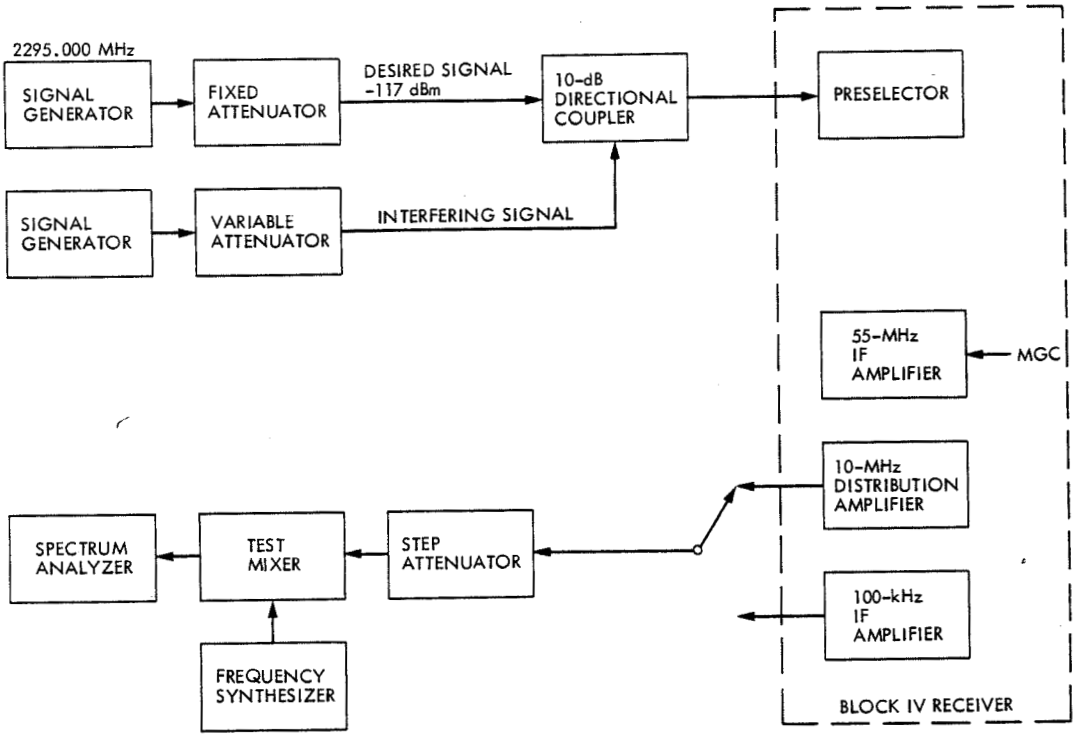


Fig. 6. Test configuration for Block IV receiver S-band saturation test

Appendix A

Equations for Maximum Allowable CW Interference Power

The equations for each segment of the graph shown in Fig. 5 are given below. In the following equations, P is the maximum allowable RFI power at the maser input in dBm, and f is the frequency of the RFI. The region of carrier tracking loop degradation is approximately 20 kHz wide with lower and upper frequency bounds of f_1 and f_2, respectively. It follows then that f_1 is f_c -10 kHz and f_2 is f_c +10 kHz. If it is desired to use these equations to protect the entire DSN receive band (2290-2300 MHz), set f_1 and f_2 to 2290 and 2300 MHz, respectively.

P = TBD for $f_1 \leqslant f \leqslant f_2$ (tracking degradation region)

P = -90 for $2270 \leqslant f < f_1$ or $f_2 \leqslant f < 2300$

P = -90 + 0.6 (2270-f) for $2170 < f \leqslant 2270$

P = -90 + 0.6 (f-2300) for $2300 \leqslant f \leqslant 2400$

P = -30 + 0.1 (2170-f) for $1870 \leqslant f \leqslant 2170$

P = -30 + 0.1 (f-2400) for $2400 \leqslant f < 2700$

P = 0 for $f < 1870$ or $f \geqslant 2700$

Appendix B

Model Assumptions

Gain Values to Circuit Points

Circuit point	From preselector input, dB	From maser input, dB
2	–	48
3	-2	46
4	-9	39
5	46	94
6	17	65
7	62	110
8	50	98
9	92	140

Conditions

(1) Signal level control set to obtain 17 dB gain from circuit point 2 to circuit point 6.

(2) Gain of 55-MHz IF amplifier = 30 dB.

Assembly Bandwidths*

Maser: 30 MHz
Preselector: 140 MHz
325-MHz IF amplifier: 72 MHz (-3 dB bandwidth)
FL3: 30 MHz
55-MHz IF amplifier: 8 MHz
10-MHz IF amplifier
  telemetry port (J6): 8 MHz
  100-kHz output (J2): 20 kHz (noise bandwidth)

*All bandwidths are -1 dB bandwidths unless specified otherwise. Roll-off asymptote slopes are available from authors.